

MEASURES TO REDUCE THE PROBABILITY OF COMPROMISES
TASK GROUP SIX REPORT

INDEX

SUMMARY	i
INTRODUCTION AND FINDINGS	1
DISCUSSION	5
RECOMMENDATIONS	16

TABS

- 1 Task Group Six Mission and Functions
- 2 The Boyce-Lee Case
- 3 The Kampiles Case
- 4 The Prime Case
- 5 The Helmich Case
- 6 The Bell Case
- 7 Summary of 21 Additional Cases Reviewed

8

9



25X1

SUMMARY

Task Group 6 was charged to study diverse recent acts of espionage ~~and~~ the output of ~~the five other integrated damage assessment task groups~~, examining the security implications and causative factors of the findings and to propose measures to help prevent security breaches in the future.* In fulfilling this assignment, representatives of CIA, DIA, NSA, and OSAF have studied in detail five recent cases of treasonable activity and reviewed ~~18~~ ²¹ other cases.

A study of several previous damage assessments and resulting recommendations for security upgrades suggests that neither a massive remodeling nor a piecemeal shoring up of the system can give a reasonable guarantee that our secrets would then be more secure. The existing system has evolved over several decades to meet changing conditions, and will continue to do so to remain effective. Those who assess as essentially sound the rules and regulations that comprise the security program are probably correct. Equally appropriate is the assessment that underscores the ultimate effectiveness of the procedures only when they are complied with scrupulously by both those charged with enforcing personnel, information, and physical security and those within the system who can observe adherence or violation of the rules. *no note*

In approaching its ^{task} charge, the task group was obliged to determine where protection should be enhanced, ~~what had been the most damaging losses, what information opposition services sought, on whom they focus attention as sources, and whom we believe are likely sources in terms both of access and susceptibility to opposition service enticement.~~ ^{who is susceptible. what character & circumstances} The group also took into

* See TAB 1 for missions and functions statement

account the impacts that proposed measures to protect intelligence information and procedures could have on efficiency. The search for reasonable remedies was complicated by the awareness that security provisions must cover a wide spectrum of situations and personnel numbering from the hundreds to the tens of thousands in a staggering array of occupations and physical circumstances. No consideration was given to the costs of proposals which are considered miniscule when compared to losses occasioned by espionage.

Thus, the recommendations for making security most effective set as a goal that

- there be some standardization of security requirements and implementation throughout the intelligence ^{US G} ^{community} world to eliminate areas of particular vulnerability.
- security become a more conscious day-to-day concern of supervisors
- ~~where~~ limited security resources ~~are available~~ (e.g., ~~the~~ ^{should} capability of ~~polygraph~~), they be first applied to personnel with key access to the most sensitive programs
- ~~[the number of personnel cleared in the future for access to such sensitive programs be limited to security-manageable proportions]~~
- ~~[principles of enhanced security be extended to the less sensitive and less vulnerable programs as resources become available.]~~

A central focus for evaluation within the personnel security system needs to be established to ensure that all information bearing on an individual's security worthiness (medical, psychological, personal, financial, professional

SECRET/NOFORN

performance) is seen with regularity by the authority (whether it be a security officer or ~~preferably~~ an assessment panel) making the determination about the individual's fitness to be or remain cleared..

In reviewing ~~retrospectively~~ both the private and professional lives of the five men who engaged in espionage, it is clear that they suffered from maladjustments. ~~[While it is unlikely that poor adjustment would be directly equated with security violations, it can serve to alert those in positions of responsibility to take some corrective action.]~~ Signs of immaturity or instability, especially when coupled with stress such as a financial problem (a common factor precipitating cooperation with an opposition intelligence service), are a cause for security concern.

~~people~~ Our study indicates that the ~~perpetrators~~ ^{Spies} of espionage ~~often~~ ^{try to} volunteer ^{this} ~~rather than~~ ^{instead of being full pay to run by h.s.} are recruited by hostile services. In all cases the treasonable activity was initiated after access to classified material had been granted, suggesting that a metamorphosis had occurred, a change to which supervisors and co-workers should have been attentive, and which calls for a program of continuing security assessment.

Nowhere does the "weak link" theory have more relevance than in security considerations. And a weak link seems to be the wide variation in security requirements ^{provision} to determine the suitability of candidates for access ~~to~~ ^{more rigorous} sensitive material. Access that would be denied by the ~~strictest~~ screening ~~(and stern assessments)~~ required by CIA or NSA for their employees could be granted elsewhere in the Intelligence Community

25X1

SECRET/NOFORN

In the British espionage case considered here* limitations of security policy appear to have played the greater role in failure to detect espionage over a 10-year period ^{rather} than faulty operation of the system. In the US cases covered here, ^{despite the use of better security procedures} lax or ~~routine~~ observation and application of ~~more~~ adequate security regulations was responsible in part in failure to discover treasonable activity. [The message of this report is that US security regulations more rigorously observed and enforced require largely only updating to account for or use new technology or techniques now available.]

25X1

The physical measures which might be taken to eliminate illegal document reproduction or removal (the primary means by which espionage was committed) are so onerous they would unacceptably obstruct the carrying out of normal required business. Therefore, this study proposes some improvement in physical safeguards to deter illicit acts, but places major emphasis on the proper and continuing assessment of personnel to determine suitability for access and continued access to sensitive materials. Throughout the study, ^{the} diligent implementation of security regulations, especially by supervisory personnel, is stressed.

The recommendations also feature wider application of polygraph procedures and psychological assessment than currently in use by many intelligence organizations.

* See Tab 4

SECRET//NOFORN

Because our study of these cases indicated that some of the individuals had "second thoughts" after becoming involved in illegal activity, the study of a ^{four} ~~short-term~~ amnesty program is proposed ^{for} ~~whereby~~ those who voluntarily ^{of course, implied in the Gov.} confess espionage activity ~~be subjected to lesser penalties in return for full cooperation.~~

Other measures proffered to reduce the incidence of espionage involve the universality and uniformity of regulations governing sensitive materials, additional research on human assessment and new ~~technology germane to~~ ^{physical} security. The task force participants also ^{recommended} ~~felt that~~ additional effort to ^{enhance} ~~make more~~ effective existing rules regarding the monitoring of foreign travel and foreign national contact, and after hours ⁱⁿ ~~(access)~~ or lone access to sensitive materials ~~[should be pursued]~~.

SECRET//NOFORN

SECRET/NOFORN

INTRODUCTION AND FINDINGS

The task group studied the lives and careers of five men - ~~four Americans~~ and ~~a Briton~~ - who engaged in treason, to determine the elements contributing to behavior and the institutional factors that facilitated the espionage. In addition to the three cases studied by the other task groups participating in this assessment, this task group elected to add two other cases that it felt demonstrated (a) the role thoughtless management can play in abetting espionage, and (b) the apparently innocuous circumstances that can lead to recruitment by an alert foreign agent. The conclusions reached from this research as to measures that would help prevent future compromises were further tested by reviewing 21 other incidents of espionage.*

The review of circumstances in the five espionage cases**: Boyce-Lee, Kampiles, Prime, Bell and Helmich make clear that the prevailing security environment failed to ^{detect this gap} ~~subject these individuals to closer security scrutiny,~~ even though warning indicators were present. The indications ranged from severe financial problems, unexplained affluence, frequent foreign travel, stressful personal and family problems, unusual work patterns, changes in lifestyle and aberrant behavior, to association with foreign nationals and known criminals, and the use of drugs. Despite the presence of one or more of these indicators in each case, they failed to ^{trigger more} ~~trigger more than routine~~ ^{any action} ~~observation.~~

It is apparent that existing security regulations, if scrupulously implemented by security-conscious personnel, could have drawn attention that

* See TAB 7

** See TABS 2-6 for case summaries

SECRET/NOFORN

SECRET/NOFORN

all was not well in most of these cases. Frequently supervisors were not alert to their security obligations and some apparently limited their responsibility to "getting the job done" without reference to the implication of that attitude on employees. In those cases where supervisory personnel did note aberrant behavior, the system failed to carry through to an alerting stage where professional security officers would become involved. Inadequate interpretation of, exceptions to, or lax enforcement of existing security regulations played a role in each of the US cases reviewed.

The perpetrators of treasonable acts did not appear to consider themselves in any great danger of discovery, at least in the early stages of their criminal activities. The security systems to which they were subject did not effectively create a perception of risk that served to deter them. Indeed, as it turned out, the security programs of their parent organizations played no role in discovery of the espionage.

The task group is also struck by the fact that there is little consistency in the sets of security requirements that apply to personnel having equal access to sensitive materials in various governments, government agencies, and industrial facilities. A very real weak link in overall security, negating a vigorous application in some organizations, arises from these disparate security requirements and enforcement.

25X1

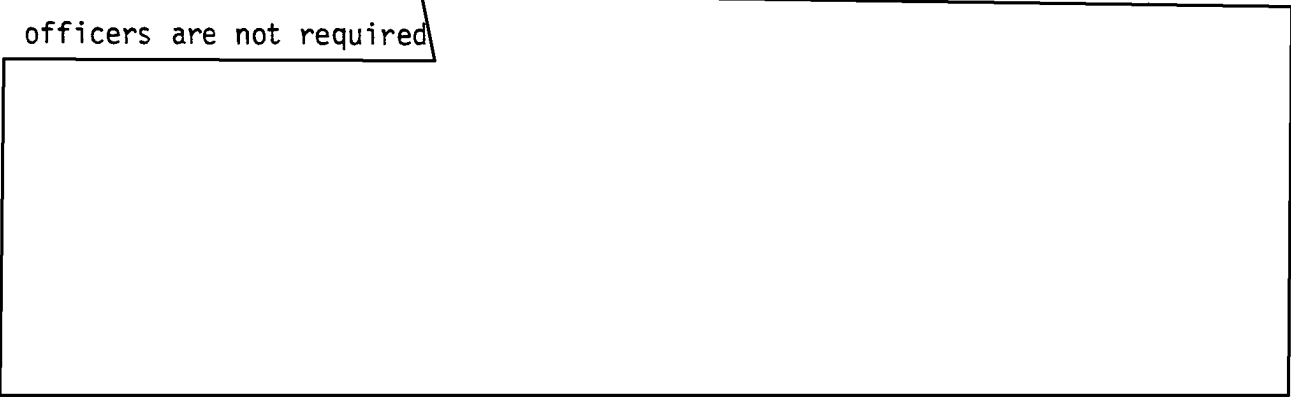
[REDACTED]

[REDACTED] DIA does not employ the polygraph in its clearance procedure, NSA polygraphs its civilian employees and contractors, but only selected military, while CIA uses the polygraph for all ^{associates} ~~employees~~. Some industrial contractors are subject only to a background investigation; others are sub-

SECRET/NOFORN

SECRET/NOFORN

jected to a polygraph examination, some prior to employment, others only after having been exposed to details of sensitive projects. Furthermore, where the polygraph is used there is general acceptance of the counterintelligence examination, ^{became} ~~but~~ lifestyle inquiry generates considerable controversy concerning invasion of privacy. The security of sensitive material is diluted where relatively strict rules for access and caretaking imposed on US intelligence officers are not required



Another weakness of the security system stems from failures to pool relevant personnel security information on an employee or applicant. Quite different judgments on employment or assignment might be reached if all of the medical, personnel, and security information were available to one evaluator or an assessment panel. The fragmentation of such information in the interests of the individual's privacy denies adequate appraisal for security purposes. Where rigorous periodic security reviews and updates of personnel and facilities are not accomplished, the changed circumstances and attitudes of personnel are not brought to the attention of professional security officers.

In studying these cases it became increasingly evident that to some degree emotional instability or immaturity was present. Some appear to have had longstanding psychological maladjustment; others were unable to cope with growing stress. There is little evidence that these instabilities were

SECRET/NOFORN

brought to the attention of or registered as a concern with supervisors, although it appears that these ^{these conditions frequently appear in the set end} conditions can be linked to the acts of espionage. Improved screening tests and standards to determine basic personality defects and developing psychological aberrations are required to assist in identifying ^{the who are potential spies} troubled personnel.

The act of espionage was accomplished in each case by the passing of documents that had been removed from a "secure" facility. The proliferation of intelligence materials and reproduction facilities has, ~~without question~~, ^{existing} ~~and outmoded~~ overtaxed accountability systems, minimizing the risk that a purloined document will be detected. The determined thief can easily avoid detection ~~of his action at this time~~. ^{Efficiency of the} Limitations imposed by security concerns vie with the need for easy access to copy machines to accomplish authorized missions. ^{invariably overcome security considerations.}

A common ^{cause} precipitant of cooperation with opposition intelligence services was ~~financial considerations~~. In all but one case the individuals initiated, ~~on their own~~, contact with the opposition service. Only one -- the ~~British~~ ^{of GCHQ} Prime case -- was a ~~preplanned~~ penetration by an already committed agent.

These facts inexorably draw attention to the need for a continuing security assessment of individuals as a first-line effort to ^{defect unsuitable personnel} ~~quell misfeasance~~ and strict enforcement of personnel as well as information and physical security to deter espionage.

SECRET/NOFORN

DISCUSSION

Diverse as the cases examined may seem, the common thread that runs through them is that existing security conditions allowed access to classified material by persons who should not have been able to acquire access and failed to detect those who, once given access, ^{understand undetected changes} ~~became affected in some way~~ that led them to acts of espionage.

The aim of the Intelligence Community personnel security procedures is to provide reasonable predictions of the reliability of the persons to whom national security information is entrusted, while continuing to give constitutionally-mandated privacy and freedom to the individual. The contention between these two imperatives of security and liberty is inescapable.

To determine the proximate causes of and to propose security improvements to help prevent or attenuate espionage in the future, five recent cases were studied.

Christopher BOYCE and Andrew LEE sold CIA contractor (TRW) data to the Soviets for personal gain. Childhood friendship, joint drug use, and greed for money established their bond. Boyce accessed the CIA material through employment at TRW. Lee transported the copied material to the Soviets.

Motive:	- Money (More than \$80,000)
Circumstances:	- Volunteered
Geographic factors:	- Contacted Soviet Embassy, Mexico City
Security weaknesses:	- Immaturity noted during BI, access adjudicated ^{routinely} at a low

SECRET/NOFORN

~~level without senior review~~

no polygraph, lax supervision

absence of search program,

worked alone in SCI/crypto vault

Access:

- Worked as document clerk, courier and communicator in TRW vault area, physically removed documents from work

Detection:

- Discovery resulted from Lee's detention and search by Mexican authorities for loitering in vicinity of Soviet Embassy.

William KAMPILES stole a KH-11 manual while a dissatisfied CIA Operations Center employee. After resigning from CIA, he traveled to Greece and sold the document to the Soviets, hoping to then regain CIA employment in the capacity of a CIA double agent operating against the Soviets.

Motive:

- Self aggrandizement/egocentric desire to work as "CIA spy" (accepted \$3,000)

Circumstances:

- Voluntary act

Geographic factors:

- Contacted Soviet Embassy, Athens

Security weaknesses:

- ~~Immaturity~~ ^{Personality flaws} evident in hiring phase, supervisor conflict/job dissatisfaction, absence of search program

? not really surfaced

SECRET/NOFORN

- Access: - Watch Officer ^{assignment} employment in CIA
Operations Center afforded access
to documents, one document physi-
cally removed
- Detection: - Contrived efforts to offer serv-
ices as double agent led to
investigation and discovery of
true circumstances of contact
with Soviets.

Geoffrey Prime offered his services to the Soviets while
assigned to a RAF SIGINT unit in Berlin. Insecure, lonely,
sexually inadequate, ~~seemingly amoral~~, and socially a misfit,
he sought to associate himself with a greater cause. For self-
rationalized reasons, he offered his services to the Soviets to
aid the "cause of socialism." Later, as a GCHQ specialist, he
operated as a Soviet penetration agent and passed sensitive data
on ~~and~~ derived from [] technical collection programs.

- Motive: - Ideology (However, accepted
\$8-10,000 in payments from
Soviets)
- Circumstances: - Volunteered
- Geographic factors: - Contacted a Soviet Military
Checkpoint in Berlin
- Security weaknesses: - Inadequate BI, no polygraph,
no psychological/psychiatric
screening, no search program
- Access: - A civilian specialist at GCHQ
clear to over to COMINT & SAT

Detection: - ^{Criminal}~~Civil~~ misconduct (sexual assaults on juveniles) led to questioning, followed by confession to wife under stress, and discovery resulting from comments by wife.

Joseph HELMICH resorted to the sale of sensitive cryptographic materials to obtain quick cash to settle debts. Insensitive management pressure (^{military superior}~~supervisor~~ demanding indebtedness be corrected within 24 hours) triggered the initial act in 1963, which led in turn to a two-year "cash for secrets" relationship with the Soviets. As a US Army communications officer, Helmich provided the Soviets with unique access to crypto equipment and communications.

Motive: - Money (More than \$130,000)

Circumstances - Volunteered

Geographic factors - Contacted Soviet Embassy, Paris

Security weaknesses - No follow-up on unexplained and sudden solvency, no follow-up on refusal to take polygraph, no search program, worked alone

Access: - Direct access to cryptographic materials and communications, physically removed materials from work

Detection:



25X1

SECRET/NOFORN

25X1

[REDACTED]

Army CI evaluation pointed toward Helmich who had refused in 1964 to take a polygraph to resolve financial inquiries. Later FBI interviews and polygraph led to partial confession.

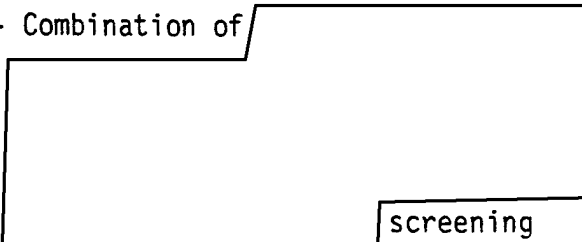
William BELL was spotted and recruited by Polish Intelligence at a time when he needed money, had experienced a middle-aged lifestyle change, and indicated some job dissatisfaction. His case typifies the vulnerability of someone in financial difficulty who, when confronted with the opportunity for seemingly easy cash at little risk, can rationalize his actions to suit his situation. Ready cash for a few documents solved his financial problems but locked him into an espionage relationship that he at first rationalized as little more than industrial espionage. Employed by Hughes Aircraft Company for 30 years as a radar engineering specialist, he had access to Secret level DoD and contractor documents revealing technical data on developmental and advanced military weapons systems, components and associated technologies, which he sold to Polish Intelligence.

Motive:	- Money (More than \$110,000)
Circumstances:	- Recruited
Geographic factors:	- Once recruited, intelligence meetings were held abroad
Security weaknesses:	- No awareness/follow-up on sudden solvency. ^{No} Inadequate BI, no ^{NAC's only}

SECRET/NOFORN

updated security check for
current clearance, some evidence of job
dissatisfaction, search program
ineffective

Access: - As DoD contractor radar
specialist had direct access to
technical documents which he
removed from work

Detection: - Combination of  screening
of Hughes personnel, and surveil-
lance of known/suspected Polish
agent in contact with Bell. Bell
confessed when interviewed/
challenged by FBI agents.

25X1

The task group isolated a number of commonalities and circumstances that
may have facilitated or contributed to the occurrence and success of the
espionage activities.

Background Factors

Personality anomalies (All cases)
Financial considerations (Boyce, Helmich, Bell)
Thoughtless management (Helmich, Bell)

Opportunity Factors

Direct access to sensitive materials (All cases)
Able to work alone (All cases)
Documents could be physically removed (All cases)
Copying equipment could be introduced into work

SECRET/NOFORN

area (Boyce, Helmich)
Copying equipment available in work area (Prime, Bell)

Security Shortcomings

Lax implementation of security regulations (Boyce, Bell, Helmich)
Inadequate BI/SBI and updates (Bell, Helmich, Prime)
Inadequate/fragmented clearance adjudication (Boyce, Kampiles, Prime)
No package/briefcase searches (Boyce, Kampiles, Prime, Helmich)
Ineffective monitoring of travel and foreign contacts (All cases)

The data charted above take on a fuller meaning when the following quantitative findings are considered:

- o Three of the five subjects were motivated by money. All three were American. Soviet intelligence recruitment doctrine has long held that Americans are especially susceptible to recruitment on the basis of personal financial gain. This becomes an even stronger recruitment incentive in cases of indebtedness and evident greed.
- o All of the subjects held intelligence meetings in foreign countries. In all of the cases constituting an established intelligence relationship, meetings were held in foreign countries to exchange classified materials and/or to conduct training in espionage techniques. In the remaining case, Kampiles committed his single act of espionage while abroad.
- o All five of the subjects physically removed documents and sensitive materials from their places of work. Absence of spot checks or package/briefcase inspections in all but one case facilitated this activity.

SECRET/NOFORN

SECRET/NOFORN

o All five passed data directly available from their official jobs. In all cases, it was not necessary for the subjects to elicit sensitive data or documents from other sources. Access was direct as a result of their work. One removed data for which he was not cleared.

o Three of the five evidenced concern/avoidance of the polygraph. Boyce turned down a CIA employment offer because of the polygraph requirement. Helmich refused to submit to an Army polygraph during investigation of his affluence. Prime stated he would not have taken a job with GCHQ if it had required a polygraph examination. (Cases other than the ^{se}five examined also indicate the deterrent effect of the polygraph.)

o The security recommendations flowing from these cases concentrate upon measures to decrease the probability of approving potential security risks for access to national security information and upon measures to help discover those who ^{not} ~~were~~ undetected by the initial screening, or who have subsequently become security risks or espionage agents.

The basic security instrument in the personnel security screening process is the background investigation, a technique originally prompted by concern over subversion and disloyalty. The security concerns today are not quite the same. Now such factors as latent immaturity, ^{egocentricity} instability, mid-life crisis and financial consideration ^{can be contributors} ~~are the~~ likely causes of treasonable behavior. Despite this changing nature of the security problem, the background investigation remains the first line of defense. The Intelligence Community has evolved a

SECRET/NOFORN

SECRET/NOFORN

common standard of investigative scope and adjudictive guidelines for access to sensitive compartmented information in the provisions of DCID 1/14.

Both CIA and NSA have found ~~that~~ a sophisticated polygraph program, an invaluable investigative aid that furnishes significant information not normally attainable by any other means, ^{The pg} is invaluable in establishing true identity, and ~~augments~~ ^{beneficially} the background investigation. The initial polygraph examination assists in screening out those not suitable for access to classified materials while subsequent examinations are effective means to detect ^{or deter} espionage. For those departments and agencies that utilize "life-style" and counterintelligence polygraph as a screening tool, the program has provided the major part of the information leading to adverse security decisions.

There are other useful augmentations to the screening process with which NSA, CIA and DoD intelligence elements have useful experience. Psychological assessment tests, which in some agencies may lead to psychiatric interviews, provide valid and useful insights into the personality of the applicant or employee.

When information derived from all these investigative techniques -- the background investigation, polygraph, psychological testing, psychiatric interview -- is pooled for panel review, a more complete profile of the individual emerges and the likelihood is increased that flaws and problem areas not fully developed by one discipline will be ^{appropriately considered} revealed.

^{to be analyzed by another discipline}

These techniques are equally valid for the periodic reinvestigation and rescreening of previously approved personnel. People change, undergo stress, suffer career frustrations, and are buffeted by family and societal problems.

SECRET/NOFORN

SECRET//NOFORN

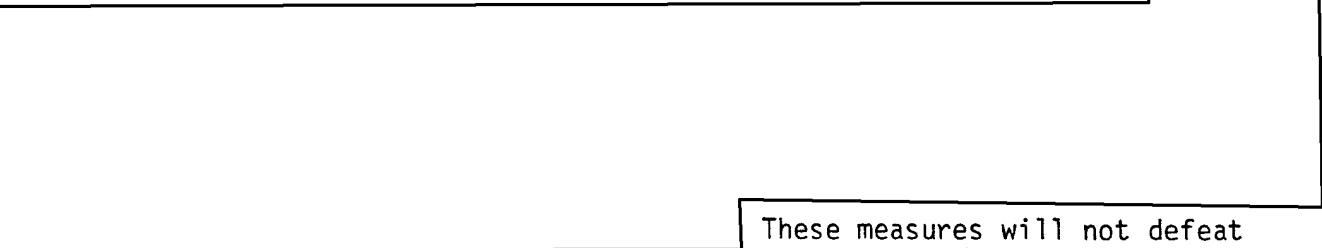
Financial pressures or latent immaturity may erupt and alter the picture of the previously well adjusted and acceptable employee. A combination of ~~these~~ investigative and screening techniques, coupled with a prudent adjudication of the "whole person", can serve both to deny access to the unsuitable and to give the Community greater assurance that cleared individuals continue to warrant access.

While the screening and periodic rescreening of employees is essential, the necessity for management, especially first-line supervisors, to be conscious of the welfare and problems of their subordinates cannot be overstressed. It is neither envisaged nor desired that supervisors become amateur therapists or security officers; it is necessary that they become more aware of employees' problems with a view toward jointly solving them.

To prevent or discourage espionage by those who evade the personnel security barriers, physical and procedural security barriers are needed. From the BOYCE case came the Intelligence Community's "two-person rule" [~~for industrial contractors~~] which directs that in areas containing large volumes of sensitive documents, no fewer than two cleared personnel must be on duty when classified material is accessible. The KAMPILES case caused CIA to reinstitute its random baggage check. (In all five cases unauthorized copies of classified documents were made in the office, or originals were removed for copying.)

25X1

There are sophisticated techniques, either in concept or in research --



These measures will not defeat ^{would} those who are really bent upon espionage at any price, but ^{would} act as deterrents to

SECRET//NOFORN

those who have escaped the personnel screen and who are leaning toward or being pressured into committing espionage.

Those with access to sensitive cryptologic information in the cases under consideration recognized the potential value of such information to an opposition service and made haste to furnish ^{such into} [either key cards or tapes] to their foreign handlers. Cryptographic procedures eliminating or restricting dependence upon such easily removable or copyable key material will become increasingly important ^{as a result of} ~~as we move~~ into the computer revolution in data handling.

25X1

25X1

Approved For Release 2005/08/16 : CIA-RDP96B01172R000300020008-0

Approved For Release 2005/08/16 : CIA-RDP96B01172R000300020008-0

RECOMMENDATIONS

Existing security practices failed to deter espionage in each of the five cases studied or detect such activity when it occurred. In addition to remedying lax administration and observation of current security rules, these recommendations are designed to enhance the system, making it more likely to discourage espionage and to surface for remedial action potential security risks and security violators.

The recommendations cover both broad aspects of security: how to deal with applicants for security clearances to screen out the unsuitable; and procedures, controls and safeguards to be applied to cleared personnel and their work environments. In all cases emphasis is on efforts to assure rigorous observance of security regulations throughout the system.

It is recommended that:

- o a universal standard of security regulations be uniformly applied to all persons accessing classified materials. ? DCI scope ?
- a. Under DCID 1/14, the DCI should enforce throughout US government agencies and their contractors identical requirements, including those for polygraph procedures for future access to sensitive compartmented information.

c.

25X1

25X1

25X1

- o Throughout the US Intelligence Community uniform security standards for access to ~~classified~~ materials be applied with consistency and constancy.
 - a. Multidisciplinary investigative procedures, BI, medical and psychological examination, and polygraph (preferably life style) be employed with an appraisal panel assessing applicants.
 - b. A continuing security assessment program using a multidisciplinary panel be rigorously enforced with periodic BI and, until adequate capabilities are available, random counterintelligence repolygraph.
 - c. Periodic credit checks be conducted on accessed persons. ?
 - d. { Waiver or relaxation of access regulations by Senior Officials of the Intelligence Community be minimized. } source?
- o The security responsibility of supervisors for their subordinates be enhanced by training and by fuller participation in periodic reinvestigation and security reevaluation of their subordinates. ?
- a. Supervisory and management training courses include specific security awareness phases including the need to be alert for indications of employee distress and to arrange appropriate counseling to avoid deterioration of the situation and increased vulnerability.

- b. Supervisors with their constant and continuing contact with subordinates be members of the panel performing the periodic security suitability evaluation and reinvestigation of employees.
- c. A systematic means of reporting to appropriate security, medical, and personnel authorities by supervisors and co-workers be developed and promulgated.

717
..

U

To ensure the implementation and effectiveness of these recommendations and to provide a continuing effort to upgrade and improve security, the DCI is urged:

- o to ~~provide~~ ^{encourage the continuing} authority(ies) and ~~funding~~ for substantive research into development of personality/psychological profiles suited to applicant and employee screening to detect both unsuitable employment candidates and high-risk employees.
- o to provide authority(ies) and funding to continue or expand research to develop copy-resistant materials and document "tags" to detect unauthorized removal.
- o to promote accelerated efforts by NSA to achieve upgrading of US cryptographic systems to a "paperless key" environment, i.e., full electronic crypto keying with tamper-proof/resistant components.
- o to ~~upgrade~~ ^{encourage} joint research efforts by agencies in the Intelligence Community into counterpolygraph training capabilities of opposition intelligence services, assessment of US polygraph

vulnerabilities to such techniques, and countermeasures development.

25X1

o

- o to convene, under auspices of the SECOM, appropriate representatives of the US Intelligence Community and the Department of Justice to explore the feasibility of some form of "amnesty program." ^{in esp for full coop.} Such a program could provide a means for persons to turn themselves in without necessarily exposing themselves to the criminal charges of espionage activity, and ^{could} ~~would~~ have a substantial "chilling" effect on opposition intelligence services targeting US persons.

In addition to the initiation of the aforementioned items, suggestions developed in previous security reviews remain valid and should be implemented. Of particular relevance to this Integrated Damagement Assessment are the following proposals that should have widespread application in the Intelligence Community.

- o screen probationary employees on reaching eligibility for career status through a combined review by the career service, ~~OMS, OS and OP.~~ ^{Mar Per Sec}
- o to the extent practicable locate and operate copy machines ^{not per} to ensure that controlled documents and copies are properly registered.
- o institute random baggage checks. ^{at all the atm glen out}
- o improve monitoring of foreign travel/contacts. ^{how!}